CLAIMS

What is claimed is:

1. A system for journaling activity in a data processing system comprising:
a sensor for capturing atomic level events; and
an aggregator, for accepting multiple atomic level events and generating a journal event.

2. A system as is claim 1 wherein the journal events are associated with a particular executing process.

3. A system as is claim 2 wherein the executing process is associated with a particular user.

4. A system as in claim 1 additionally comprising:
a filter for filtering atomic level events with an approved event list.

5. A system as is claim 4 wherein the approved event list includes a list of approved file identifiers.

6. A system as in claim 4 wherein the file identifiers are a hash code.

7. A system as in claim 1, wherein the sensor is located within a client agent and the aggregator is located within a server.

8. A system as in claim 7 additionally comprising:
a coalescer for coalescing atomic events output by the sensor prior to inputting them to the aggregator.

9. A system as in claim 8 wherein a bundle of coalesced events is created prior to their transmission between the agent and the server.

10. A system as in claim 8 wherein sequence numbers are added to bundles.

11. A system as in claim 1 wherein a journal event is detected as a suspect action with a data file.

12. A system as in claim 1 wherein an event is attributable to a known user, thread and/or application as identified at a known time.

13. A system as in claim 8 wherein the coalescer reports an event after a time out period with no activity.

14. A system as in claim 1 wherein journal events are used to control security of the data processing system.

15. A system as in claim 1 wherein the journal events are used to provide a perimeter of accountability at a point of system use.

16. A system as in claim 15 wherein a point of use is a user desktop and accountability is of data files.

17. A method for journaling activity in a data processing system comprising:

capturing atomic level events; and

aggregating multiple atomic level events to generate a journal event.

18. A method as in claim 17 additionally comprising:

filtering atomic level events with an approved event list.

19. A method as in claim 18 where the approved event list includes a list of approved file identifiers.

20. A method as in claim 17 wherein the step of sensing atomic level events is located within a client agent and the step of aggregating multiple atomic level events occurs within a server.

21. A method as in claim 20 additionally comprising:

coalescing atomic events output by the sensing step prior to providing them to the aggregating step.

22. A method as in claim 21 where a bundle of coalesced events is created prior to a step of transmitting them between the client agent and the server.